COMPUTER DATA SECURITY

Dale Leslie Larson

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA 93940

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

COMPUTER DATA SECURITY

by

Dale Leslie Larson

June 1974

Thesis Advisor: G. L. Barksdale, Jr.

Approved for public release; distribution unlimited.

T 161050

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
Computer Data Security

5. TYPE OF REPORT & PERIOD COVERED
Master's Thesis
June 1974

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Dale Leslie Larson

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93940

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93940

12. REPORT DATE
June 1974

13. NUMBER OF PAGES
59

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)
Naval Postgraduate School
Monterey, California 93940

15. SECURITY CLASS. (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Data Security
Computer Security
Access Security
Security Verification System

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)
This thesis presents a wide spectrum of computer data security, including both practical and theoretical aspects of the subject. It was motivated by the concern for the general lack of adequate knowledge, techniques, implementation, and application of computer data security. The objective was to (1) review the pertinent features of data security and the relationship of these features to the

Block #20 continued

computer and its users; (2) generate an awareness of the techniques and problems in data security by presenting the main issues; and (3) discuss theoretical as well as specific applications of techniques and methodology for data base security and data access control. The intention was to present to everyone concerned - from the manager to the computer expert - the necessity for computer security and some of the forms which it may take.

Computer Data Security

by

Dale Leslie Larson
Lieutenant Commander, United States Navy
B. S., Naval Postgraduate School, 1973

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 1974

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA

ABSTRACT

This thesis presents a wide spectrum of computer data security, including both practical and theoretical aspects of the subject. It was motivated by the concern for the general lack of adequate knowledge, techniques, implementation, and application of computer data security. The objective was to (1) review the pertinent features of data security and the relationship of these features to the computer and its users; (2) generate an awareness of the techniques and problems in data security by presenting the main issues; and (3) discuss theoretical as well as specific applications of techniques and methodology for data base security and data access control. The intention was to present to everyone concerned - from the manager to the computer expert - the necessity for computer security and some of the forms which it may take.

TABLE OF CONTENTS

I. INTRODUCTION..... 9

II. NATURE OF THE PROBLEM..... 11

A. HISTORICAL ASSESSMENT..... 11

B. SCOPE OF DATA SECURITY..... 12

C. COMPUTER ENVIRONMENT..... 14

1. Multi-Level Data..... 14

2. Multi-Programming..... 14

3. Multi-Processing..... 15

4. Multi-Level User..... 15

5. Remote Terminal Access..... 16

D. DATA SECUIRTY THREATS..... 17

1. Accidental..... 17

2. Deliberate..... 17

E. COMPUTER ABUSE..... 19

F. PRIVACY..... 21

III. DESIGN AND APPLICATION OF DATA SECURITY..... 24

A. THEORY OF PROTECTION..... 24

B. PROTECTION MECHANISMS IN MULTICS..... 26

C. DATA ACCESS CONTROL MECHANISMS..... 27

1. Memory Level..... 28

2. Process Level..... 28

3. Logical Level..... 30

D. AUDIT AND SURVEILLANCE TECHNIQUES..... 32

E. CRYPTOGRAPHIC APPLICATION..... 33

IV. PHYSICAL AND ADMINISTRATIVE DATA SECURITY..... 37

A. PHYSICAL SECURITY..... 37

B. ADMINISTRATIVE SECURITY..... 39

V. A DATA SECURITY MODEL..... 40

A. THE PHYSICAL MODEL..... 40

B. THE PROCEDURAL MODEL..... 44

C. THE MATHEMATICAL MODEL..... 47

VI. CONCLUSIONS..... 53

APPENDIX A..... 55

LIST OF REFERENCES..... 57

INITIAL DISTRIBUTION LIST..... 59

LIST OF FIGURES

1. Access Control Matrix..... 25
2. Ring Protection Structure..... 30
3. Privilege Control Matrix..... 31
4. Security Verification System..... 43
5. Security Property Determination Matrix..... 50

ACKNOWLEDGEMENT

The author wishes to express his appreciation to Professor Gerald L. Barksdale, Jr., for his guidance and assistance with the formulation, organization and content of this thesis. Special thanks go to my wife Corky, for her understanding and typing assistance.

I. INTRODUCTION

One of the most difficult problems confronting the computer industry today is that of data security. The problem is one which involves the manufacturer, operator, and user, and encompasses physical facilities, operational procedures, computer hardware, software, and programming techniques. The computer is rapidly emerging from its childhood status to take its place as an indispensible part of our modern society. The more dependent we become on the computer's abilities and the more significant its work becomes, the more important it is to protect the computer from those who would misuse its power. The problem of computer data security is expressed by Peter S. Brown [Ref. 1]:

> "The computer has unleashed countless opportunities for industrial growth, activity, new applications, labor-saving accomplishments, improving the quality of decisions and many others. At the same time, computer technology has spawned a whole new field of crime and generated a series of problems for both designers and users of information systems."

Our social, political and technical lives are rooted in an information-based society with an expanding need for collecting and storing information. Most recently, even our private lives have been touched by this ability to collect and propensity for accumulating large data bases. It is generally agreed that the effective use of information provides the capability for an organization to improve its

efficiency of operation. However, the advent of computers did not initiate the desire for information gathering nor did it create the data security problem. Organizations have always collected information and then had the problem of its security. Computers have enlarged the scope of information gathering, allowing greater and greater quantities of information to be collected, recorded and retrieved at high speed. The problem lies in the fact that computer based centralized information systems contain large amounts of easily accessible data, making intrusion and compromise profitable. Any effective data security system must have as its ultimate goal the methodology for ensuring that the value of the information is not worth the effort required to obtain it.

The objective of this thesis was to (1) review the pertinent features of data security and the relationship of these features to the computer and its users; (2) present the main issues in data security so that an appreciation and awareness of the techniques and problems involved can be easily grasped; and (3) discuss theoretical as well as specific applications of techniques and methodology for data base security and data access control.

Good [Ref. 26] has said, "Information is a unique asset in that it can be stolen but may never be missed (in contrast to a physical asset)." For this reason, protection of information is an insidious business and will require much of our intelligence and technology to successfully accomplish.

II. NATURE OF THE PROBLEM

A prerequisite to solving a problem is a clear understanding of the problem itself; computer data security is no exception. The intent of this section is to present the computer data security problem with respect to its origin, development, and present environment. Analysis is presented relative to the abuse and privacy infringement of computer data, and the threats against data security.

A. HISTORICAL ASSESSMENT

Historically man's quest for obtaining information and data has been the basis for innumerable tales of intrigue, deception, and ingenuity. History can be segmented into eras delimited by what has been called "data-handling revolutions" by Kahn and Prywes [Ref. 2 and 3]. The first data handling revolution began around 1650 with the institution of regular intercity postal services. Shortly thereafter, government groups often called "black chamber operations" were organized to illegally collect the information. They would intercept the mail, extract useful information, re-seal the letters, and send them on without the sender's or receiver's knowledge. The next data handling revolution began with the introduction of the telegraph about 1850. Again government organized groups, as well as commercially sponsored teams, were used for the illegal interception, decoding, and distribution of telegraphic

messages. The third data handling revolution commenced around 1895 with the introduction of the radio. Presently we find ourselves a few years into a major technological revolution in data handling involving computers. Historically then, it is not surprising to find individuals and organizations involved in the work of illegally obtaining, manipulating, destroying, or in some way compromising computer based data. A projection of historical developments indicates that we should expect a growing trend of well financed and organized activities to attempt to gain access to secure data.

B. SCOPE OF DATA SECURITY

The scope of data security can be as wide and complex as the data the system is designed to protect. It can range from a simple lock on the door of the computer room to the use of sophisticated hardware, software, and crypto-graphic techniques. Techniques for security also include programmed routines, manual procedures, and physical means using security personnel, locks, keys, badges, voice prints, and hand prints. The International Business Machine Corporation [Ref. 4] defines data security as follows:

> "Data security can be defined as the protection of data from accidental or intentional disclosure to unauthorized persons and from unauthorized modification."

This definition was taken from a widely distributed IBM monograph on data security which was instrumental in focusing

attention on the problem. Another definition comes from Clark Weissman [Ref. 5] who states that:

> "Security of computer based data systems is the prevention of (1) unauthorized gain of information or system access, (2) denial of authorized access, and (3) data or service falsification."

The techniques of data security must be applied across the total automatic data processing (ADP) system in order to be effective. This total system can be classified into six specific elements: (1) physical environment, (2) people, (3) communications, (4) policies and procedures, (5) hardware, and (6) software. In its broadest sense, data security is involved with the storage of removable storage media, such as magnetic tape reels, magnetic disk packs, input cards, and output listings. Additionally, programmer and electronic data processing controls, auditing personnel selection, and employee security are related to data security. Yet another category of data security is the physical protection measures such as guard services, alarms and locks, closed circuit television, and bugging devices. Also related to data security are techniques in data processing as in data checking, maintaining backup files, alternate processing facilities in case of equipment malfunction, and program testing and software verification. Lastly, part of computer data security is the legal controls and insurance safeguards for software protection, trade secrets and copyrighted material.

C. COMPUTER DEVELOPMENT

Data security is a function of the level of data that is to be protected. Its security is also dependent upon and dictated by the environment in which the computer is operated, and the data transmitted. One of the reasons that data security has become such a problem to the computer industry is the numerous ways a computer and its data are employed.

1. Multi-Level Data

In an environment of multi-level data, the computer system contains data with various levels of classification, such as: UNCLASSIFIED, CONFIDENTIAL, SECRET, and TOP SECRET. A scheme of hardware and/or software must be employed to handle these different levels of data. The system must maintain the mutual disjunction between the different levels and still allow reasonable access by authorized users. A non-homogeneous data bank significantly increases the number and complexity of controls required to ensure data security.

2. Multi-Programming

The technique of multi-programming produces an environment which permits more than one job to occupy the computer at the same time. Since the possibility exists that each job may be at a different level of classification, the security system must provide for compartmentalization with no possibility of intersection during simultaneous main memory occupancy. There are a number of computer data

security systems which provide some measure of partitioned main memory. The MULTICS system is one of these and will be discussed later.

3. Multi-Processing

Multi-processing is a system that includes more than one central processing unit (CPU). In a multi-processing system, each CPU operates independently of one another primarily to increase system throughput or reliability. The CPU's share information by using the same main storage and by using the same input/output devices. Where main storage is shared, usually the same routines are used and the same queue of jobs serviced. According to Katzan [Ref. 6], multi-processing represents a serious potential data security problem, since a program executing in one CPU can utilize the same locks and keys used in one of the other CPU's. Specifically, the threat to data security is due to the common utilization of security controls and memory between CPU's, and the simultaneous occupancy of memory by programs using different levels of data. This condition reflects a degradation in the mutual disjointness of information segments required for a secure data system. Consequently, a more complex system of hardware and software is required to maintain data security in an environment of multi-processing.

4. Multi-Level User

At most computer installations, each user is given some level of security clearance. These classes can be as

many and as varied as desired, however, most organizations follow closely the military's system of UNCLASSIFIED, CONFIDENTIAL, SECRET, and TOP SECRET. The military goes a step further and bases individual access on a two parameter function, the first being the level of clearance, and secondly a "need to know" associated with the specific data. The result is a unique set of users for each specific piece of data. In computer data security, a further restriction to the data access authority of the user is the type of access allowed, such as read only, write, append, grant further access, execute, delete, etc. A discussion of the theoretical and actual implementation of data security for a multilevel user via an access control matrix format will be discussed in sections III and IV.

5. Remote Terminal Access

A large share of the problems in data security involves time and resource sharing remote terminal systems. Since many users have access to the system, identification and authorization security systems are needed. A system which allows users to share the direct-access storage facilities dynamically must provide a data security system that prevents one user from accessing another user's data. Since data must be sent between terminal and computer, some form of secure communication must be an integral part of any data security system. User identification and authorization, data storage, data integrity, and secure data transmission will be discussed in detail later.

D. DATA SECURITY THREATS

The underlying principle of data security is to prevent data from being compromised. The reason for the wide range of security techniques employed today is that data compromise can occur in various forms and under numerous conditions. Petersen and Turn [Ref. 7] classify the threats to data security as being accidental or deliberate.

1. Accidental Threats

The major portion of any computer data threat discussion usually involves deliberate infiltration; however, the consequences from accidental disclosure of sensitive information could be just as costly and serious as an incident in which deliberate means were used to gain data access. Accidental disclosures of data could be as a result of hardware failures, software errors from poorly designed or only partially debugged programs, or operational errors such as mounting the wrong magnetic tape or magnetic disk pack. Accidental threats are insidious in nature but can be considered logically as a proper subject of deliberate threats. Therefore, the remainder of this section will be devoted to the deliberate threats to computer data.

2. Deliberate Threats

Deliberate infiltration implies a plan or purpose with preconceived objectives in mind. Carrol and McLelland [Ref. 8] list their objectives of deliberate infiltration as: (1) gaining access to information in files; (2) discovering the information interests of users; (3) altering

or destroying files; and (4) obtaining free use of system resources. Petersen and Turn [Ref. 7] further classify deliberate efforts to gain information as passive or active.

Some deliberate passive threats are caused by electro-magnetic radiation from computer hardware and communications equipment by observation of data traffic at some point in the system. Passive methods include electromagnetic pickup, wiretapping, and information obtained from concealed transmitters. One of the least guarded against and most productive deliberate passive techniques is to examine periodically the contents of the waste containers in and around the computer or remote terminal area. It is not uncommon for copies of partially working programs and lists of input and output data to find their way into the most convenient waste receptacle.

Most of the data security techniques and countermeasures are directed against deliberate active threats asserts Katzan [Ref. 6]. These threats are similar for all computer data systems and differ primarily in the degree to which a specific system design feature allow exploitation. Deliberate active threats includes the following:

a. Browsing involves the use of legitimate access to the system to obtain unauthorized information.

b. Masquerading

This is the practice of obtaining proper identification through improper means, such as wiretapping, and then accessing the system as a legitimate user.

c. Detection and Use of Trap Doors

The trap doors are hardware features, software limitations, or specially planted entry points that provide an unauthorized source with access to the system.

d. Entry via an Active Communications Channel

Penetrating communications channels involves intercepting messages between a user and the computer ("piggy back"), entry via the communication lines of an inactive user ("between-lines entry"), and canceling a user's signoff signal and then continuing to operate under his password and authorization.

e. Physical Means of Entry

This method includes access to the system through a position with the computer center, a communications company, or a vendor, the generation and analysis of "core dumps", and the theft of removable storage media.

E. COMPUTER ABUSE

Parker, Nycum, and Oura of the Stanford Research Institute [Ref. 9] have compiled and conducted an extensive study on computer related crime. They define computer abuse as any act associated with computers where victims have suffered or could have suffered a loss and perpetrators made or could have made a gain. There are numerous cases in the courts today concerned with breaches of computer integrity. An expert from Anderson and Company, the CPA firm, estimated recently annual losses from computer thefts in the neighborhood of a billion dollars, [Ref. 3].

Fraud, theft, larceny, embezzlement, vandalism, extortion, the crimes are the same, only their environment is changing. The computer and its automatic data processing functions are becoming the setting for today's large scale frauds. Perpetrators of these frauds and thefts need the skills, knowledge, and access associated with computers and data communications technology.

Many of the computer frauds read like science fiction and are presented here only as an indicator of what is happening today and the potential of what may occur in the future. An analysis of computer related crimes is given by Parker and Nycum [Ref. 10]. The first programmer convicted for stealing programs was in 1964 for which he received a five year prison term. The first federal criminal case occurred in 1966 when a 21 year old programmer put a patch in his program to ignore his own checking account in checking for overdrafts. The first documented case of stealing a program from the memory of a computer over telephone circuits and a remote terminal occurred in 1971. Some recent cases of computer fraud include the $1.5 million New York Union Dime Bank embezzlement, the $2 billion Equity Funding Insurance fraud, the $1 million Los Angeles Telephone Company equipment theft and the $300,000 Long Island and Pittsburg Westinghouse embezzlement.

The emergence of the "Robin Hood syndrome" (taking from from the machines which control society) and the "skyjack syndrome" (where crime becomes popular) with respect to

computers has generated an apathetic public attitude toward computer data security. Parker believes that in order to control and prevent computer related crime, ethical standards and applicable laws must be established, and that technological solutions are necessary, but not sufficient.

F. PRIVACY

The concept of "womb to tomb history" for each individual made possible by the computer's vast storage capacity and rapid retrieval capability is frightening to many people. The Federal Government has at least twenty-seven agencies and bureaus gathering information, much of which is quite private and personal [Ref. 11]. Some of these agencies and bureaus are the Census Bureau, the Customs Bureau, the Naturalization Service, the Department of State, Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and Department of Commerce. Employers gather personal information on prospective employees, as well as banks, credit card companies, doctors, lawyers, and educational institutions. The idea of a centralized, cross-referenced, easily and quickly available master file on each individual is technically possible. A total "identifier" on a master file, indexed through a single identifying number (S.I.N.) is both a temptation and a threat. The advantage of S.I.N. in time saved, cost reductions, and overall accuracy to organizations such as the police, banks, life insurance companies, Internal Revenue Service, employers, doctors, and educators is obvious

and real. In terms of individual and institutional liberties, S.I.N. poses a potential of serious consequences including direct infringement on basic liberties. Large centralized computer data banks using a single identification number as the total identifier for an individual do not yet exist; however, the idea is technically feasible and economically sound. The development of centralized record keeping seems almost inevitable.

Much of the potential for protection and security of data banks is contained in the basic structure of the computer itself. Its speed, accuracy, and storage capacity make the computer its own best protector. Until recently, computer access data security had been geared toward the protection of industrial and political information. Computer data banks containing sensitive information on an individual basis must protect the human right to privacy. The "right to know" or "freedom of information" must be measured against an individual's "right to privacy." The United States Constitution in its Bill of Rights guards against specific invasion of privacy in the matters of religion, speech, unreasonable search and seizure, and self-incrimination; no mention is made as to what extent individual privacy may be abridged for the good of the public. The new technology is computerized data banks has opened up new areas of challenge to the basic problem of privacy.

Hurley [Ref. 11] reports that the Department of Health, Education, and Welfare (HEW) has summed up a proposal for

safeguarding personal information by including in its draft report on the subject that, "The application of automated data processing technology to the records containing personnel data can be subjected to appropriate and effective social constraint without diminishing its usefulness." In the final analysis, the legislative, judicial, and executive branches of government, in conjunction with private enterprise, must work together in formulating the attitudes, climate, and background necessary to solving the problem of computer invasion of privacy. Self-regulation and self-restraint cannot in itself provide for the guarantee of individual privacy throughout the ADP environment. A legal framework relating directly to computers and data banks seems to be the inevitable answer. A summary of the main elements of present and proposed data privacy laws is contained in Martin [Ref. 12, pages 437 to 446]. The laws and safeguards of a computerized society may require that other computer provide the checks and balances necessary to ensure the environment of informational privacy we require and desire.

III. DESIGN OF THE COMPUTER DATA SECURITY SYSTEM

The purpose of this section is to review some concepts of data security and discuss principles, methods, and techniques of data security that are independent of any particular system. An actual study of a proposed system is discussed in section V entitled, "A Data Security Model."

A. THEORY OF DATA PROTECTION

A theory of protection is discussed by B. W. Lampson [Ref. 13] and establishes a method for controlling access to the objects of a process in an operating system environment. A second paper by Graham and Denning [Ref. 14], is based on Lampson's work and presents a formal model of the concepts and principles of protection theory. Both of these papers are concerned with operating system structure and hardware architecture, while the security verification system (SVS) proposed in section V suggests security isolated from the computer's operating system.

Lampson describes the computer's capabilities and resources as a set of "objects" protected by the system's hardware and software. An operational environment is created for each user which appears as a virtual machine. The objective is a protected executing program which is conditioned such that it: (1) does not destroy the operating system files or memory space; (2) will not invade other program's

domain; (3) can be shared among other system users; and (4) may invole another program and share its data files.

Graham and Denning [Ref. 14], approach data security from seven different levels of protection of the operating system. These levels range from complete isolation of programs or data files to providing "certified" subsystems whose correctness has been completely validated and guaranteed. The objective of Graham and Denning's work is to present a structure of protection mechanisms that are effectively independent of the computer system and of internal program structure. The design of their system involves the specification of objects, subjects, and protection rules so that every attempt by a subject to access an object must be validated by the protection system. As displayed in Figure 1, we define matrix A, with subjects as rows and objects as columns. Matrix A contains attributes that describe the access privilege of subject S_i to object O_j, such that S_i would have A_{ij} access to O_j. A_{ij} is some attribute (read only, write, etc.) and P = program, F = file, D = device, and so on.

	OBJECTS				
	O_1^P	O_2^F	O_3^D	$\cdots O_j^Z \cdots$	O_n^X
S_1	-	-	-	...	-
S_2	-	-	A_{23}	...	-
:					
S_i	-	-	-	A_{ij}	-
:					
S_m	-	-	-	...	-

Figure 1. Access Control Matrix.

The particular operational environment determines the manner in which the above concepts of protection theory are implemented and the degree of protection provided. Normally the hardware/software protection system is transparent to the user and is governed by the rules of the actual implementation. It should be noted that though the protection systems briefly presented here are theoretical in nature, they form the basis for many of the methods of data access security presently being designed or in use.

B. PROTECTION MECHANISMS IN MULTICS

Whenever computer data security is discussed, particularly in the area of secure data sharing, the MULTICS system is usually mentioned; MULTICS is an acronym for Multiplexed Information and Computings Service. MULTICS is a prototype computer utility developed as a result of an ADVANCED RESEARCH PROTECTS AGENCY sponsored research program. The goal of the MULTICS project [Ref. 15] has been to produce a general purpose programming system that provides a large and diverse user community with: (1) remote terminal access as the normal mode of system usage; (2) continuous service; and (3) large amounts of on-line data storage with controlled secure sharing of information among users.

Unlike nearly all commercially available systems, the controlled information sharing of MULTICS was an initial design goal and the mechanisms to achieve this goal were built-in from the very beginning. The protection mechanism

is essentially a hardware addressing mechanism and a hardware implemented mechanism for dividing a computation into multiple regions of different accessibility. Specifically, the MULTICS hardward implements an access control ring structure (see process level, page 26), in the following two ways. First, the hardware controls the access checking logic, and via the segment addressing hardware, validates each virtual memory reference. Secondly, the hardware contains instructions for changing the ring of execution. The results of this hardware based system have been a method which protects files from unauthorized use while providing secure data sharing.

Systems which have attempted to provide data security as an after thought (after hardware design) via software implementation have had only limited success in comparison to the hardware oriented system of MULTICS. This implies that a successful data security system should be an initial design goal of the hardware, which is substantiated by Weissman in [Ref. 16]. Corbato [Ref. 17] provides an overview of the MULTICS system, including its protection features and presents a bibliography of available documents on the system. A detailed description of the protection hardware in the new MULTICS processor is given by Schroeder and Saltzer in [Ref. 18].

C. DATA ACCESS CONTROL MECHANISMS

The purpose of data access control mechanisms in a computer system is to protect private data from compromise

while providing the mechanism to allow regulated access to shareable information. David Hsiao [Ref. 19] views data access control mechanisms from three levels; (1) memory level, (2) process level, and (3) the logical level.

1. Memory Level

The memory level access control mechanisms control access to memory in terms of units of memory. The protection of the system is with respect to the segments of memory, not the segments contents. The contents of each segment of memory are subject to the same access controls that govern each memory unit and are protected only as long as they remain within the same memory unit. A typical physical memory protection scheme employs memory bound registers or storage protection keys which control access to bounded memory areas.

2. Process Level

A process is simply a set of programs with its associated data. Therefore, process protection and control is concerned with access to and protection of programs. An elaborate process access control mechanism known as the "ring mechanism" was proposed by Graham [Ref. 20] and is depicted in Figure 2. This concentric ring mechanism allows one program to give control to another without violating any of the access control rights of either program. Conceptually the concentric ring mechanism requires the user to arrange his processes hierarchically, where processes at the lower part of the hierarch (outer ring) have less privileged access rights.

Each process has a fixed number of domains (protection rings). The rings are distinguished by integers 0 through n-1 (for MULTICS, n = 7). The ith ring contains the access capabilities of rings i + 1, i + 2, ..., n-1, and forms a proper subset of rings i - 1, i - 2, ..., 0. The sets of access capabilities represented by the various rings form a collection of nested subsets with ring 0 the largest and ring n-1 the smallest set in the collection. The result of this hierarchical system of rings is that protection provided by a given ring of a process is effective against procedures executing in higher numbered rings. Having multiple domains of protection generates the need to change the domain of execution of a process. Changing the domain of execution may also change the capabilities available to a process and, therefore, must be controlled. The control over the domain change is keyed to certain program locations called gates, shown in Figure 2. Changing the domain of execution must occur only as a result of a transfer of control to one of the gate locations of another domain. If the transfer is not directed to one of the gate locations, the transfer is not allowed. The use of separate access control gate location lists for each data file and separate descriptor files for each process will provide the means to control separately the use of each data file by each user's process.

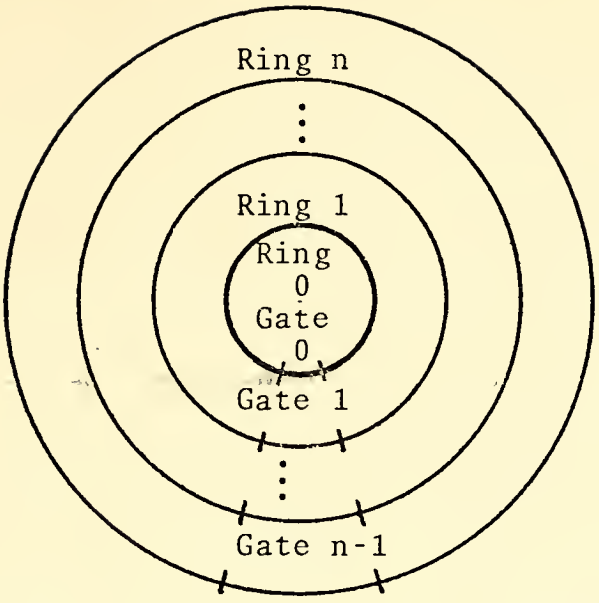


Figure 2. Ring Protection Structure.

3. Logical Level

The third, and highest level of access control is the logical level. A user will generally structure his data in terms of logical units such as field, records, and files. Unlike memory levels of access, here the logical units of information have little resemblance to their physical or virtual storage images. By allowing the user to associate access control requirements and protection measures with logical units, the access control mechanism can facilitate direct control and protection of the information regardless of its physical location.

If we let the type of access a user has to the data base be represented as an authority item, then the entire collection of authority items can be viewed as an access control matrix. Allowing the rows of the matrix to represent users and the columns the logical units of data, as shown in

Figure 3, then the entry A_{ij} contains a series of access privileges and restrictions held by users i to logical unit j. NOTE: F_j = File, r_j = Record, f_j = Field, A_{ij} = Read only, Write, Delete, Own, etc.

If A_{ij} is blank, access to the logical unit is denied.

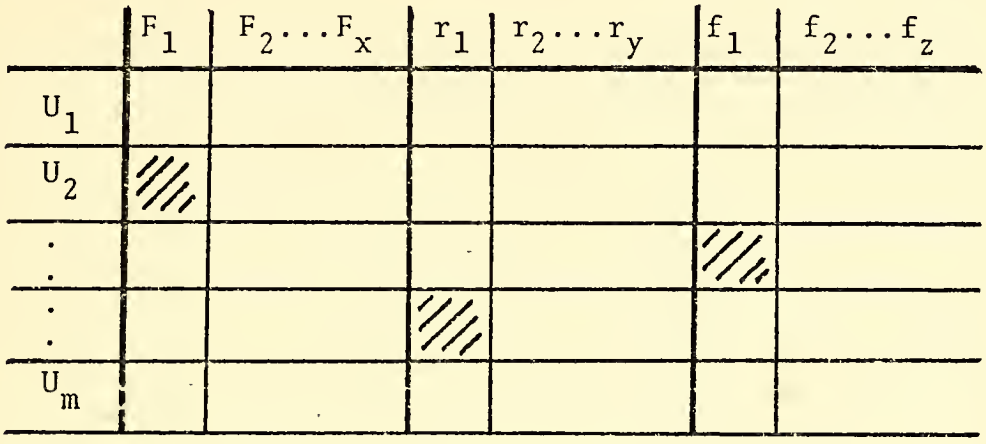


Figure 3. Privilege Control Matrix.

For actual implementation, the matrix is too sparse and, therefore, would be uch to expensive in terms of space to be stored as depicted in Figure 3. Since access privileges and restrictions to the same data units differ from one user to another, and since there are usually more data types than number of users, the implementation should be user oriented. Specifically, there should be one set of authority items per user. The matrix in Figure 3 is essentially the same as that of Figure 2 on page 30, except that Figure 3 is user (U_j) oriented and Figure 2 is process (S_i) oriented.

In addition, the set $\{F_i, r_i, f_i\}$ of Figure 3 is a subset of the set $\{0_i\}$ of Figure 2.

D. AUDIT AND SURVEILLANCE TECHNIQUES

Auditing and surveillance techniques can provide immediate warnings of illegal system penetration or a posteriori data security protection. Monitoring can be performed so that it is known to the infiltrator or transparent to him, with each attempt to violate the system's security or data files recorded for subsequent analysis. One approach is to delay termination of a user after several attempts to access an unauthorized segment of data, but report the attempted infiltration to the computer operator or security officer for appropriate action.

Surveillance and monitoring can be performed at various levels depending on the classification of data being protected and security requirements of the system. Some system violations can always be expected due to user accidents. If the expected number of violations increases rapidly, it is reasonable to assume that deliberate penetration attempts are being conducted. Conversely, if the expected number of violations decrease markedly, there might be reason to believe that some means of illegally accessing the system has been discovered. Data security is a dynamic function which depends on the kind of data stored and the usage patterns of the users that access it. The maintenance and use of security logs is a means of detecting the need for a change in the data security requirements or methods.

E. CRYPTOGRAPHIC APPLICATION

The best computer security system devisable can be rendered totally useless by simple wiretapping techniques during classified data transmission. The best-known and most widely used techniques to provide security for data transmission and to protect sensitive data files are called privacy transformations. The use of cryptographic systems can effectively counter the wiretapping threat through encoding (enciphering) data prior to transmission and then decoding (deciphering) after data reception. Data files can be stored in the enciphered form to provide even greater protection against compromise.

The basic cryptographic process is a set of rules which comprise the system which transforms "plain" or "clear" text into the "cipher" text and then back to the original text again. Katzan [Ref. 6] defines three main classes of general cipher systems: (1) transposition systems, (2) substitution systems, and (3) algebraic systems.

A transposition cipher system is one which the characters of the plain text data are rearranged in some prescribed manner. The characters maintain their identity while losing their positional significance. Transposition ciphers can usually be easily implemented on a digital computer with reasonable efficiency; however, they are relatively unsophisticated and easily broken.

The substitution cipher system involves the replacement of plain text characters by other characters. Here the

plain text characters lose their identity but usually maintain positional significance. In its simplest form, a substitution cipher uses two alphabets, one containing the characters of the plain text data, the other comprising the respective cipher equivalents.

An algebraic cipher is a system which replaces the plain text characters with numbers using some deterministic scheme and then performs some reversible series of mathematical operations on these numbers.

Ciphers need not be restrained to single system for their generation. Use of a digital computer for encoding and decoding data allows numerous cipher systems to be combined in a complex cryptographic system which is both fast and virtually error free. Van Tassel [Ref. 21], lists four criteria that could be applied to the design of a cryptographic system: (1) it should not be necessary to keep the method secret-only the keys; (2) the amount of secrecy obtained should be directly related to the amount of computing time necessary to use the system; (3) the system should destroy the statistical parameters of the natural structure of the language; and (4) an error should not destroy successive information.

The Vernam cipher system, invented in 1917 by Gilbert S. Vernam, is particularly applicable to a computer based data system. This cipher uses a pseudo-random number generation scheme for its key. The Vernam cipher uses the "exculsive or" operator so that if the plain text were

10011 and the key were 01001, then the encipherment would be 11010.

This system is particularly convenient since all digital computers use the binary digits 0 and 1 to represent its characters, most digital computers have an "exclusive or" operator, and encoding and decoding are reciprocal operators. Originally, Vernam used a tape of random binary digits, however, it was soon shown that periodic keys were subject to decryption. The infinite key method presented by Carroll and McLelland [Ref. 8], is a technique for use with the Vernam cipher. This method uses random numbers generated by a pseudo-random number generator, usually available on most general purpose computers, with the seed being an N-digit password. The method "exclusively or's" random keys with the characters of a plain text data, exactly as in the Vernam cipher. By manipulation of the seed after N-random keys are generated (where N is the maximum period of the generator), any number of characters can be enciphered. Now all that remains is the synchronization of the activities on each end of the data line. This is usually done by establishing a set of variables (seeds) for the generator and transporting the information between sites by carrier or registered mail. Later, all a message need provide is an indexing number into the particular set of variables to be used in the generation process. Thus, effective synchronization can take place for each data set that is to be enciphered or deciphered.

The foregoing section on cryptology has been presented as a quick overview of a vast subject with only one specific application to a computer environment. Employment of cryptographic techniques is an absolute necessity where the security of transmission lines cannot be guaranteed and the classification of data warrants the additional time and cost. For additional references on cryptology relative to the computer environment, the reader is directed to Appendix A.

IV. PHYSICAL AND ADMINISTRATIVE DATA SECURITY

The theoretical and technical controls discussed in section III can be effectively negated without the proper physical and administrative controls. Wasserman [Ref. 22] suggests that physical security is needed on all aspects of the data processing operation. The physical protection required in computer systems is similar to that required for conventional office spaces. Computer installations raise a few special problems, such as the control of electromagnetic devices, wiretapping, electrical supplies, and air conditioning. Administrative security has the responsibility for the security techniques and procedures in the day-to-day computer operation. It is generally agreed that the weakest link in any computer data security system is the people who operate the system. The responsibility for personnel security clearances, and of employee attitude and conduct with respect to data security, is a function of administrative security.

A. PHYSICAL SECURITY CONTROLS

Martin [Ref. 12], separates physical security into three layers of defense. First the perimeter barrier such as a wall or fence. Second, the walls, windows, doors, and ducts of the building itself. Third, locked cabinets and vaults. A perimeter defense, if not guarded by some means, will act only as a psychological deterrent to some intruders, but have

little effect on the determined intruder. A perimeter defense that is guarded will offer the protection mentioned above as well as an early warning of the presence of the determined intruder. Well-secured doors and windows are essential to good building security, thus they should have associated alarm devices. The would-be intruder will likely enter by some non-alarm controlled passage, such as manholes, storm drains, utility tunnels, the roof, or through a common wall. The combination of electronic detectors and a randomly roving guard force can greatly enhance building security. The inner layer (locked cabinets and vaults) of defense becomes important simply because it is the last line of defense between the determined intruder and the data. The security of safes, cabinets, and store rooms is often neglected on the naive assumption that the other two layers will keep out intruders.

A large portion of an organization's data security plan is based on backup tapes for recovery and re-initialization. These tapes may prove useless if stored in an unsecure method. Whether the storage area is a safe, vault, or designated room, it must be resistant to burglars, fire, water, heat, humidity, and explosion. Reliability is the prime factor in a security system. The reliance on faulty security equipment builds in a false sense of security which can be disasterous. Validation of the reliance of security equipment must be accomplished through ongoing tests which measure equipment function against minimum standards criteria.

B. ADMINISTRATIVE SECURITY CONTROLS

Responsibility for the strategy and methodology of physical security belongs at the highest level of management in an ADP system. A computer system's security officer should have the responsibility of the following: (1) overall security coordination; (2) procedural controls; (3) controls on programs and programmers' physical security; (4) external administrative controls; and (5) security system audits. In addition to his responsibilities for physical security, the security officer may be the only person who can access the system's authorization tables, determine access authorities for programs and data, issue passwords, and ensure correct operation of the data security system. Finally, the security officer should have the responsibility for investigation of security violations, review of security audit records, security training, and assessment of the effectiveness of the security techniques employed.

V. A DATA SECURITY MODEL

The following data security model is presented not as a working mechanism, but as a first step toward a secure computer data system. A system utilizing multi-level data, multi-programming, multi-processing, multi-level users and remote terminal access is assumed.

A. THE PHYSICAL MODEL

The literature is full of ideas, schemes, and mathematical models developed for the purpose of user identification, data access control, file privacy protection and new file classification. All these proposed protection plans seem to pre-suppose that the protection system will be an integral part of the main computer's operating system. Making any software protection system part of the operating system creates immediate deficiencies and problems, such as: (1) increase of operating system overhead; (2) allowing near access to the main system prior to any user identification; (3) no separation (logic, physical or electrical) between the protection system and the data it was designed to protect; and (4) make the security system difficult, if not impossible to prove formally correct.

If the computer's operating system has the total responsibility for system security, then its requirement for CPU time and memory will increase, allowing less time for problem directed computation. An operating system with excessive

overhead will have low efficiency as exhibited by its poor thruput. Secondly, an unidentified user should not be allowed entrance to the operating system for the purpose of determining identification and data access control level. All determination of authorization and access authority should be made independent of and prior to actual system connection. Once an illegal user has gained entrance to the operating system, it is much easier for him to circumvent the security controls. Thirdly, as a principle of good security, there should be a buffer between that which you are trying to protect and the protection system. Lastly, the complexity of logic and the large number of instructions in an operating system make it highly susceptible to undetected penetration, trap doors, modification, and system errors; in addition, it will be virtually impossible to prove its correctness. Allowing the data security system to reside as an integral part of the computer's operating system will result in an overhead and cost per job increase, efficiency decrease, and a degradation in the level of overall data security.

These considerations suggest the need for a separate, virtually independent system for user identification and data access control. It is proposed that all or as much of the security responsibility as possible be delegated to a separate, independent mini or micro computer system which will hence be referred to as a "Security Verification System" (SVS). The SVS has marked advantages, not the least

of which is low cost. The standard mini or micro-computer system even with additional storage media, is in the few thousand dollar range vice hundreds of thousand dollars range of a large general purpose computer. A SVS interfaced with a large general purpose machine, as depicted in Figure 4, would not increase operating system overhead, but may actually reduce it. This is true because many of the file access decisions could be made independent of and prior to actual access of a specific file by the operating system. Using a SVS would keep a user separated from the main data banks until his identification, authority, category, and need to know relative to the specific files and library programs was determined and authenticated. The SVS would make all the determinations as to user identification and data access control. The computer's operating system would merely respond to a "go", "no go" decision and service the authenticated user within the limits and areas prescribed by the SVS. Utilizing a SVS as described above would allow physical, electronic, and logical separation between the data, CPU, and main memory, and the data security system designed to protect and control access to them. Using a small special purpose mini or micro computer security verification system would make the system correctness more easily proved because of its narrowness of purpose and relative simplicity.

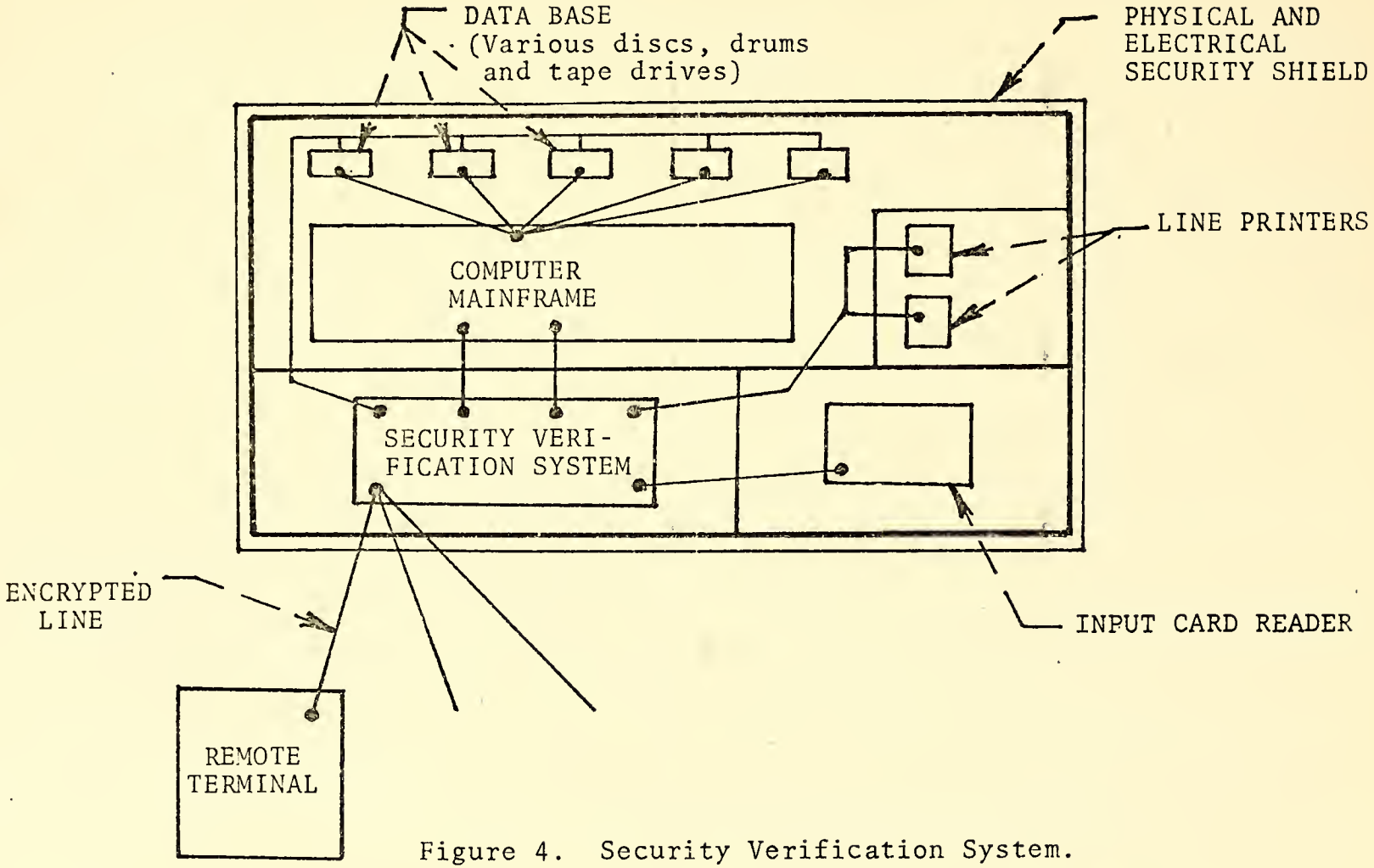


Figure 4. Security Verification System.

B. THE PROCEDURAL MODEL

User identification using the SVS can be made as simple or as extensive as the data being protected dictates. The following is merely one possible user identification scheme, parts of which utilize already existing and implemented methods, other parts having been proposed by various authors in the literature and the remaining parts are original.

The initial login procedure would consist of typing in the user's first name, middle initial, and last name, followed by a user's identification number. This identification number need not be secret and would only be used for name/number correlation, administrative bookkeeping and auditing, and as a final entry point into the specific user's list of passwords and pertinent personal data. If the name and user I.D. matched, the SVS would ask the user to input his first, second, or third password. These passwords could be a variable length, alphanumeric string. The length of the password could be made a function of the level of data to be protected. For instance, a six character alphanumeric string would have 36^6 possible combinations. Two errors during initial login identification would sound an alarm and disallow the terminal from being connected via the SVS to the main computer. If the passwords have a uniform random distribution, the maximum probability of guessing the correct password on the first attempt would be $1/36^6$ or 4.593×10^{-10} and would increase slightly to $1/36^6-1$ for the second attempt. In order that the response to the

computer's request for a password would not appear on the typewritten teletype copy, a prefix such as $PW($PASSWORD) could be mechanized to prevent the next six input characters from being printed on the teletype paper.

Hoffman [Ref. 23] recounts Earnest's novel approach to the scheme of maintaining password integrity which is based on the assumption that an enemy is attempting to discover a user's password for his own unauthorized use, by using a wiretap or other type surveillance. The suggested method is as follows. The user logs in and identifies himself with name and user identification number (I.D.). The computer then supplies a pseudo-random number to the user who performs some simple mental transformation T on the number and then sends the results of that transformation back to the computer. The computer (in this case the SVS) performs the same transformation using a previously stored algorithm. A comparison is made of the two numbers, with equality representing authenticity of the user. The unique feature is that while the user has performed T on X (pseudo-random No.) to yield Y = T(x), any unauthorized listener, even if the information is sent in the clear, sees only the numbers X and Y. Even a simple transformation like,

$$T(x) = \left(\sum_{i=\text{odd}} \text{DIGIT}_i \text{ of } X\right)^2 + (\text{HOUR OF THE DAY}) - (\text{DAY} + X_i)$$

is almost impossible to break. A numerical example of the above method after 10:00 o'clock in the morning and before

11:00 o'clock on the 4th day of the month follows:

The computer asks: PASSWORD(34871) =

The transformations:

$$T(X) = (11)^2 + 1000 - (4 + 11) = 121 + 1000 + 15$$
$$= 1136.$$

The user responds with the number: 1136.

One time identification of a user at a remote terminal using the form described above may not be sufficient to give the desired level of protection. A periodic dialogue or random repeated interrogation of the user via the SVS may be necessary as a function of various parameters, such as, job classification, user and terminal clearance, file classification, and time on line. The SVS could ask periodically for another user password of the alphanumeric or number transfer form or the SVS could ask various questions of the user which would normally only be known by him, such as: (1) wife's maiden name; (2) date and place of marriage; (3) oldest son's age; (4) mother-in-law's birthday, etc.

The questions could come from a comprehensive questionnaire filled out by the user at some earlier time. This periodic, ongoing dialogue with the user further ensures system security and integrity. As before, two incorrect answers to any question energizes an alarm and drops the terminal off the line. Another approach to two incorrect answers would be to continue a dialogue with the suspected infiltrator while security people are alerted. This would

allow the security force to take positive action without the infiltrators knowledge.

C. THE MATHEMATICAL MODEL

Prior to the modeling of any system, certain assumptions must be made. The assumptions made above still apply. In designing security controls, particularly for a military computer system, an environment of "malicious threat" must be assumed. According to Weissmann [Ref. 24], from which much of the following model was taken, a security control system should: (1) support heterogeneous levels and types of classifications; (2) in itself be unclassified until primed with the security parameters; (3) be isolated from the total time sharing system; and (4) be relatively inexpensive. The SVS attempts to fulfill the above criteria and assumptions, while providing the security, flexibility, and growth potential required by most computer installations. Security is a total system problem encompassing hardware, software, personnel, communications, and asset physical security. In the following model, the emphasis is on the software required to implement the SVS hardware package, because in most working systems, this is the area of greatest latitude and freedom in exercising data access security control. A formal model for a software system of identification and data access control is developed.

The notion of a security object is defined as any object which has or can be assigned a level of classification or clearance, such as a user, terminal, file, job, or any other

peripheral device desired (i.e., line printer, plotter, computer controlled card punch). For notational purposes, let u denote some user, t some terminal, j some job, and f some file. Various security decisions will be made as a function of these security objects.

Next we introduce the idea of a security property. Each of the security objects is described by a security profile that is an ordered set of four elements of security properties; Authority (A), Category (C), Necessity (K), and Mode (M). The security property "Authority" is defined as the clearance of an object such the UNCLASSIFIED (a^0), CONFIDENTIAL (a^1), SECRET (a^2), and TOP SECRET (a^3) are elements which belong to the set A hierarchically ordered where

$$A = \{a^0\ a^1\ a^2, \ldots\ldots\ a^W\}. \qquad (1)$$

The security property "Category" is a set of specific compartments which are mutually exclusively sanctuaries with specific jurisdictions such as: RESTRICTED (c^0), CRYPTO (c^1), EYES ONLY (c^2), NUCLEAR (c^3), POLITICAL (c^4), INTELLIGENCE (c^5), where the Category C is the set

$$C = \{c^0, c^1, c^2, \ldots\ldots c^X\}\ . \qquad (2)$$

The security property "Necessity" (or need to know) is the set of users for each security object such that

$$K = \{u|u \text{ is a user}\}. \qquad (3)$$

The security property "Mode" indicates the type of data access required. The Mode indicates; READ ONLY DATA (m^0), ADD TO

DATA (m^1), CHANGE EXISTING DATA (m^2), DELETE FROM DATA (m^3), EXECUTE A PROGRAM (m^4) or CHANGE A PROGRAM (m^5). If we let α denote a security object, then the set M_α may contain none, any combination of or all the elements belonging to M where:

$$M_\alpha = \{m^0, m^1, m^2, \ldots . m^y \quad . \tag{4}$$

With respect to the "Necessity" property (K), it is possible to distinguish four sets of users if we allow the user u to be subscripted by the specific security object. If we let u_f^0 denote that user number 0 has access to file f and so on for the other three security objects, except that u_u^0 is simply defined as u^0, then with respect to "Necessity" it is possible to define

$$K_u = \{u\} \tag{5}$$

$$K_t = \{u_t^0, u_t^1 \ldots . u_t^\theta\} \tag{6}$$

$$K_j = \{u_j^0, u_k^1 \ldots . u_j^\phi\} \tag{7}$$

$$K_f = \{u_f^0, u_f^1 \ldots . u_f^\lambda\}. \tag{8}$$

Above, equation (5) is saying that the need-to-know for a user is restricted to himself. Equation (6) states that the Necessity of terminal t belongs to ϕ different users who have access to t. Equations (7) and (8) are similarly defined.

The matrix of Figure 5 presents the rules for determining the four security properties for a given object. An example of the rules follows. For a USER u the A_u, C_u and M_u are assigned as constants. K_u is given by Equation (5). For a

SECURITY OBJECT (α)	SECURITY PROPERTY (P)			
	AUTHORITY (A)	CATEGORY (C)	NECESSITY (K)	MODE (M)
USER (u)	ASSIGNED CONSTANT	ASSIGNED CONSTANT	u	ASSIGNED CONSTANT
TERMINAL (t)	ASSIGNED CONSTANT	ASSIGNED CONSTANT	u_t^i	ASSIGNED CONSTANT
JOB (j)	$\min(A_u, A_t)$	$C_u \cap C_t$	u_j^i	$M_u \cap M_t$
FILE (f)	ASSIGNED CONSTANT	ASSIGNED CONSTANT	u_f^i	ASSIGNED CONSTANT

Figure 5. Security Property Determination Matrix.

terminal t, A_t, C_t and M_t are assigned constants while K_t is given by equation (6). For a job, since we are given A_u and A_t, A_j is determined as:

$$A_j = \min(A_u, A_t). \tag{9}$$

Similarly then, since we are given C_u and C_t, C_j is determined as

$$C_j = C_u \cap C_t \tag{10}$$

and K_j is given by equation (7). For a file, A_f, C_f and M_f are assigned constants and K_f is given by equation (8).

The object now is for the SVS to control a user's access to a system, its terminals, and files. Access will be granted to the system if and only if u belongs to the universal set of users:

$$u \in U. \tag{11}$$

The process for user identification and authentication is described in the section of this thesis entitled, "THE PROCEDURAL MODEL," page 44.

Access is granted to a terminal if and only if the user belongs to the Necessity set for the terminal:

$$u \in K_t \ . \tag{12}$$

Now if our SVS concludes that equations (11) and (12) are true for a particular user, then it can be stated that

$$u = u_t = u_j . \tag{13}$$

Finally access is granted to a file if and only if:

1. The authority of the job is greater than the authority of the file.

$$A_j \geq A_f \tag{14}$$

and

2. The Category of the job is a superset of the Category of the file:

$$C_j \supseteq C_f \tag{15}$$

and

3. The Mode of the job is a superset of the Mode of the file

$$M_j \supseteq M_f \tag{16}$$

and

4. The user having jurisdiction over the job belongs to the set of equation (8)

$$u_i \in K_f \ . \qquad (17)$$

If expressions (14) and (15) and (16) and (17) hold true, then access is granted.

VI. CONCLUSIONS

Computer data security is a complex and many faceted problem which has only recently received general recognition. Technology has not now, nor will it ever be able to produce an absolutely secure computer data system. Technology can and must produce a system which makes it economically infeasible to compromise computer stored information. The complexity of a data security system depends on the level of data being protected and environment in which it is being used. Hardware and software implemented data security systems must be augmented by physical, administrative, and legal security techniques in order to ensure the integrity of the system.

The ultimate goal of a computer data security system is to adequately protect the data while keeping the system economically feasible and maintaining reasonable ease of authorized access. Data security involves people; people design, implement, and operate the security system to protect data from being compromised by people. Armed with the knowledge of the problem, the theoretical models, and the present technology, computer data security designers must formulate the techniques, methodology, and procedures to eliminate illegal computer data exploitation.

The following quote was taken from the WWMCCS Senior Officer's Handbook [Ref. 25]; it summarizes the motivation for this effort.

> "Currently there is no available combination of software and hardware features that can insure acceptable security when processing more than one classification/category of data in an environment other than totally dedicated. This severely restricts the capability to share computers that were designed for timesharing in the first place. To process more than one classification or category of data with existing hardware and software requires that all users be cleared for all data in the system, since there is no assurance one can access only a specified portion of a data base. The adverse implications of this limitation regarding the distributed data base concept are apparent."

Since large scale ADP systems require years in the procurement cycle, today's security problems are essentially the result of yesterday's neglect; if there is to be secure automatic data processing systems tomorrow, it will depend on what is done today.

APPENDIX A

This Appendix contains a list of reference material which pertains specifically to cryptology.

1. Brown, E. F. (editor), Computer and Software Security, New York, AMR International, Inc., 1971, p. 61-61.

2. Carroll, J. M. and P. M. McLelland, Fast Infinite-Key Privacy Transformation for Resource Sharing Systems Proc. of the 1970 Fall Joint Computer Conference, AFIPS, Vol. 37, p. 223-230.

3. Cryptology, Collier's Encyclopedia, Vol. 7, New York, Crowell-Collier Educational Corporation, 1972, p. 519-530.

4. Cryptology, Encyclopedia Americana, Vol. 8, New York, Americana Corporation, 1972, p. 276-285.

5. Cryptology, Encyclopedia Britannica, Vol. 6, Chicago, Encyclopedia Britannica, Inc., 1972, p. 844-851.

6. Feistel, H., W. A. Notz, and J. L. Smith, Cryptographic Techniques for Machine to Machine Data, Yorktown Heights, N. Y., IBM Corp. Research Division, Report No. RC 3663, December 27, 1971.

7. Gaines, H. F., Cryptanalysis, New York, Dover Publications, 1956.

8. Girsdansky, M. B. (author), Data Privacy, IBM Research Reports, Vol. 7, No. 4, 1971.

9. Kahn, D., The Code Breakers, New York, The Macmillan Co., 1967, p. 125-213.

10. Krishnamurthy, E. V., Computer Cryptographic Techniques for Processing and Storage of Confidential Information, International Journal of Control, Vol. 12, no. 5, 1970, p. 753-761.

11. Meyer, C. H. and W. L. Tuchman, Pseudorandom Codes Can be Cracked, Electronic Design, November 9, 1972, p. 74-76.

12. Notz, W. A. and J. L. Smith, An Experimental Application of Cryptography to Remotely Accessed Data Systems, Yorktown Heights, N.Y., IBM Corp., Research Division Report No. RC 3508, August 18, 1971.

13. Skatrud, R. O., A Consideration of the Application of Cryptographic Techniques to Data Processing, Proc. of the 1969 Fall Joint Computer Conference, AFIPS, Vol. 35, p. 111-117.

14. Twigg, R., Need to Keep Data Secure, Electronic Design, November 9, 1972, p. 68-71.

15. Van Tassel, D., Advanced Cryptographic Techniques for Computers, Communications of the ACM, Vol. 12, No. 12, December 1969, p. 664-665.

16. Van Tassel, D., Computer Security Management, Englewood Cliffs, N.J., Prentice-Hall, Inc., p. 121-130.

17. Van Tassel, D., Cryptographic Techniques for Computers, Proc. of the 1969 Spring Joint Computer Conference, AFIPS, Vol. 34, p. 367-372,

LIST OF REFERENCES

1. Brown, Peter S., "Computer Security - A Survey," Data Base, Vol. 4, No. 3, p. 1, Fall 1972.

2. Kahn, David, "The Code Breakers," Macmillan, p. 163-213, 1967.

3. Prywes, Noah S., "Some Problems and Consideration of Computer Security," Naval Ship Research and Development Center (NSRDC), Proceedings of the Conference on Secure Data Sharing, p. 144-152, August 1973.

4. "The Considerations of Data Security in a Computer Environment," International Business Machine Corporation, IBM-Data Processing Division, 1968.

5. Weissman, Clark, "Computer Security: Problem Dimension and Solution Space," NSRDC Proceedings on the Conference on Secure Data Sharing, p. 9, Report 4130, August 1973.

6. Katzan, H., Jr., "Computer Data Security," Van Nostrand Reinhold Company, p. 44, 1973.

7. Petersen, H. E. and Turn, R., "System Implications of Information Privacy," Proceedings AFIPS, 1967, SJCC, Vol. 30, p. 291-300.

8. Carrol, J. M. and McLelland, P. M., "Fast Infinite-Key Privacy Transmission for Resource Sharing Systems," Proceedings of the 1970 Fall Joint Computer Conference, AFIPS, Vol. 37, p. 223-230.

9. Parker, D. B., Nycum, S., and Oura, S. S., "Computer Abuse," The National Science Foundation Rahn, HSF/RA/S-73-017, November 1973.

10. Parker, D. B., Nycum, S., "The New Criminal," Datamation, Vol. 20, No. 1, p. 56, January 1974.

11. Hurley, Mark J., "The Privacy Crisis," Catholic Information Service, No. 73, p. 2.

12. Martin, James, "Security Accuracy, and Privacy in Computer Systems," Prentice-Hall, Inc., Englewood Cliffs, New Jersey, p. 437-446, 1973.

13. Lampson, B. W., "Dynamic Protection Structures," Proceedings of the 1969 Fall Joint Computer Conference, AFIPS, Vol. 35, p. 27-38, 1969.

14. Graham, G. S. and Denning, P. J., "Protection Principles and Practice," Proceedings of the 1972 Spring Joint Computer Conference, AFIPS, Vol. 40, p. 417-429, 1972.

15. Schroeder, M. D., "Protection Systems in MULTICS," NSRDC Proceedings of the Conference on Secure Data Sharing, Report 4130, p. 26-33, August 1973.

16. Weissman, Clark, "Trade-off Considerations in Security Systems Design," Data Management, p. 14-19, April 1972.

17. Corbato, F. T., Clingen, C. T., and Saltzer, J. H., "MULTICS: The First Seven Years," Proceedings AFIPS, 1972, SJCC, Vol. 40, AFIPS Press, Montvale, New Jersey, p. 571-583.

18. Schroeder, M. D., and Saltzer, J. H., "A Hardware Architecture for Implementing Protection Rings," Communications of the ACM, Vol. 15, No. 3 (March, 1972), p. 157-170.

19. Hsiao, David K., "Logical Access Control Mechanisms in Computer Systems," NSRDC Proceedings on Conference of Secure Data Sharing, Report 4130, p. 34-56, August 1973.

20. Graham, R. M., "Protection in an Information Processing Utility," Comm. ACM, 11, 5 (May 1968), p. 365-369.

21. Van Tassel, D., "Computer Security Management," Englewood Cliffs, New Jersey, Prentice-Hall, Inc., p. 121-130, April 1972.

22. Wasserman, J. J., "Plugging the Leaks in Computer Security," Harvard Business Review, p. 119-129, Sept.-Oct. 1969.

23. Hoffman, L. J., "Computers and Privacy: A Survey," Computing Surveys, Vol. 1, No. 2, p. 85-97, June 1969.

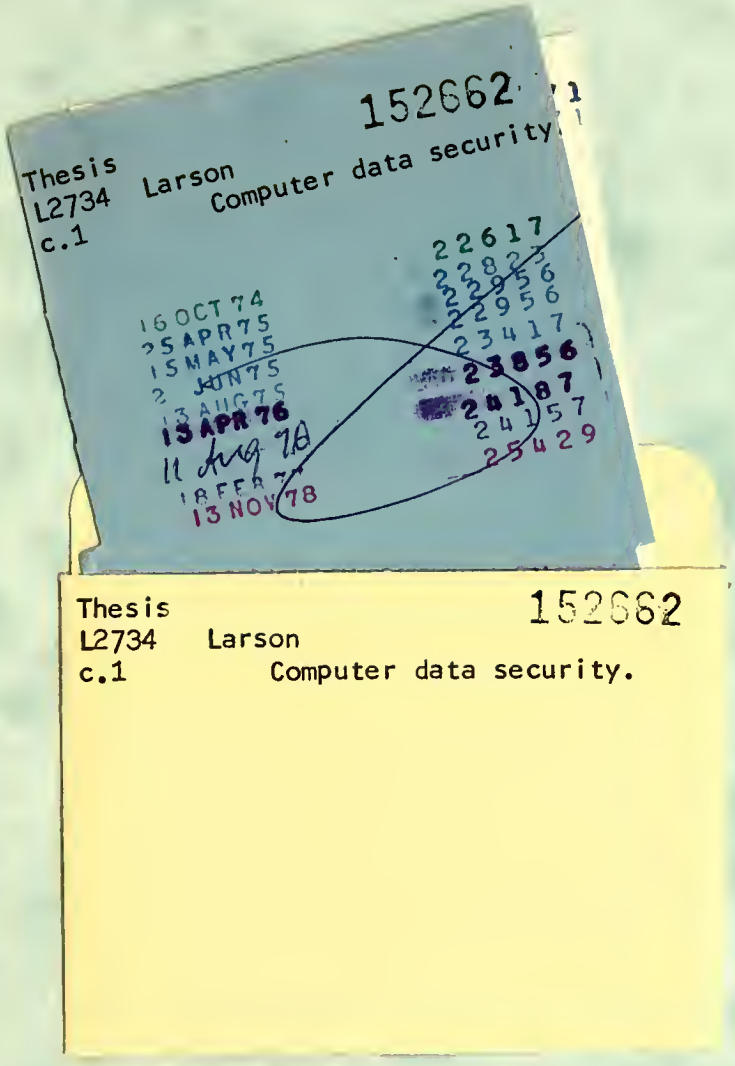
24. Weissman, Clark, "Security Controls in the Adept-50 Time-Sharing System," Fall Joint Computer Conference, Vol. 35, p. 119-133, 1964.

25. "Major Unresolved Problems," WWMCCS Senior Officers Handbook, Vol. 1, p. 3-51, 31 January 1973.

26. Good, George E., Telecommunications, Vol. 8, No. 3, March 1974, "New Developments in Data and Voice Security," p. 35-36.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Chairman, Computer Science Group Code 72 Naval Postgraduate School Monterey, California 93940	1
4.	Professor G. L. Barksdale, Jr., Code 72Ba Computer Science Group Naval Postgraduate School Monterey, California 93940	1
5.	CDR R. M. Hanna, Code 964 Fleet Material Support Office Mechanicsburg, Pennsylvania 17055	1
6.	LCDR D. L. Larson, USN 555 Poinsettia Street Chula Vista, California 92010	1


152662
Thesis
L2734 Larson
c.1 Computer data security.
16 OCT 74
25 APR 75
15 MAY 75
2 JUN 75
13 AUG 75
13 APR 76
11 Aug 78
13 NOV 78
22617
23825
22956
22956
23417
23856
24187
24157
25429

Thesis
L2734 Larson
c.1 Computer data security.
152662

thesL2734
Computer data security.
3 2768 002 12253 3
DUDLEY KNOX LIBRARY